Key HITECH Changes to HIPAA

The *Health Information Technology for Economic and Clinical Health Act* (HITECH or Act) was passed by the federal government under the *American Recovery and Reinvestment Act* of 2009. HITECH represents a historic investment in health information technology to improve the quality of health care delivery and patient care. HITECH made changes to the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), particularly with regards to strengthening the privacy and security of protected health information (PHI) and increasing the penalties for violations of HIPAA. The following chart summarizes key modifications to HIPAA by HITECH, which began to take effect in 2010.[1]

Category	Issue Modified by HITECH	HIPAA Standard	Standard as Modified by HITECH
Audits	Practice audits by HHS	Not mandatory	HITECH requires HHS to do periodic audits to ensure that covered entities and their business associates are complying with HIPAA regulation.
Covered Entity[2]	Definition of a covered entity	Health plan, clearinghouse, or provider involved in the disclosure of PHI	Expanded to include health information exchanges, regional health information organizations, e-prescribing gateways, subcontractors, and personal health record vendors.
	Is a business associate a covered entity?	No	Yes – subject to HIPAA Privacy and HIPAA Security rules. Business associates will be subject to the same HIPAA security provisions as covered entities for implementing administrative, physical, and technical safeguards on PHI. They are also subject to civil and criminal penalties for violation of these business associate requirements.
Data Breach	Data breach notification	No direct obligation, although state laws vary	Covered entities must notify patients of a breach by first class mail (or email if specified by an individual) within 60 days of discovery of the breach by the covered entity or its business associate. There are limited exceptions for unintentional access by employees and inadvertent disclosures within an office. Notification to the Department of Health and Human Services (HHS) is required. Notification is required by the covered entity to prominent media outlets if more than 500 patients affected.
	Data breach enforcement	Collaborative investigation involving HHS and a covered entity	HHS investigation to determine willful neglect[3]; expanded to include individual employees at covered entities and business associates.

[1] For additional information regarding the changes made to HIPAA by HITECH, refer to the additional resources section.
[2] Covered entities refer to groups that transmit health information electronically and are required to comply with requirements for safeguarding the privacy of protected health information; HITECH expanded the requirements of HIPAA.

Category	Issue Modified by HITECH	HIPAA Standard	Standard as Modified by HITECH
Data Breach (cont.)	Data breach penalties	Under HIPAA, the minimum penalty was $100 with a maximum of $25,000	HITECH increased fines for data breach. Fines under HITECH are $100 to $50,000 per violation, with yearly maximum of $25,000 to $1.5 million and mandatory penalties for willful neglect. The Act establishes a tiered system of civil penalties, including if the person did not know that they had violated a provision, if the violation was due to reasonable cause, or if the violation was due to willful neglect. A corrective action can be required in lieu of a penalty if the person who or entity that committed the violation is unaware that a violation occurred. HHS must investigate any complaint related to a violation that may have resulted from willful misconduct. If a violation due to willful misconduct is found, HHS must assess civil monetary penalties.
Electronic Media	Definition of electronic media	Limited to storage media, such as tape and disk	Expanded to reference Internet and VoIP technology.
Fundraising	Fundraising opt-out	If patients opt out, covered entity must make reasonable efforts to stop fundraising communications	If patients opt out, covered entity must stop fundraising communications.
PHI	Use of PHI	HIPAA states that when a practice is asked to provide PHI, they are permitted to provide only the minimum necessary information to accomplish a specific task	Under HITECH, the use of PHI is defined in more detail to enhance the privacy and security of PHI. HITECH requires health care organizations to limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set or to the minimum necessary. HITECH clarifies that the covered entity disclosing the PHI is required to make the minimum necessary determination.
	Disclosure of PHI	Organizations required to account for non-routine disclosures	Organizations that use electronic health records must account for all disclosures, including those for treatment, payment, and healthcare operations. Organizations also must account for disclosures made by their business associates or provide individuals with a list of their business associates and their contact information. HITECH shortens the accounting period from six to three years. Patients may require restrictions on disclosure of their PHI to a health plan where the patient paid out of pocket, in full, for items or services.
	Sale of PHI	Allowed	Prohibited by covered entities and business associates without valid authorization, save for certain conditions.[4]

[3] The conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

[4] Public health activities; research; treatment; services rendered by the business associate; or the sale, transfer, merger, or consolidation of all or part of a covered entity.

Category	Issue Modified by HITECH	HIPAA Standard	Standard as Modified by HITECH
PHI (cont.)	Use of PHI in marketing communications	Patient authorization required with three exceptions – covered entity services, treatment, case management/alternative treatment	Expanded to ban direct or indirect payment for communications; now applies to business associates.
	Dissemination of a patient's PHI to the patient	Only if readily available	Must be provided, preferably in electronic format; fee cannot exceed labor cost. Organizations must provide the patient (or individuals or entities authorized by the patient, such as doctors and personal health record services) with an electronic copy of their medical record.

Additional Resources

- Ambulatory Center Surgery Association, *Understanding the New HIPAA Requirements* (January/February 2010) (http://www.ascassociation.org/ASCA/FederalRegulations/HIPAA/UnderstandingHITECH)
- American Society for Healthcare Risk Management, *HIPAA after HITECH: Top 5 Issues for Physician Practices* (http://www.ashrm.org/ashrm/advocacy/advisories/files/2009hitech.pdf)
- Miaoulis, William M. Access, Use, and Disclosure: HITECH's Impact on the HIPAA Touchstones. *Journal of AHIMA* 81, no.3 (March 2010): 38-39; 64. (http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_046691.hcsp?dDocName=bok1_046691)